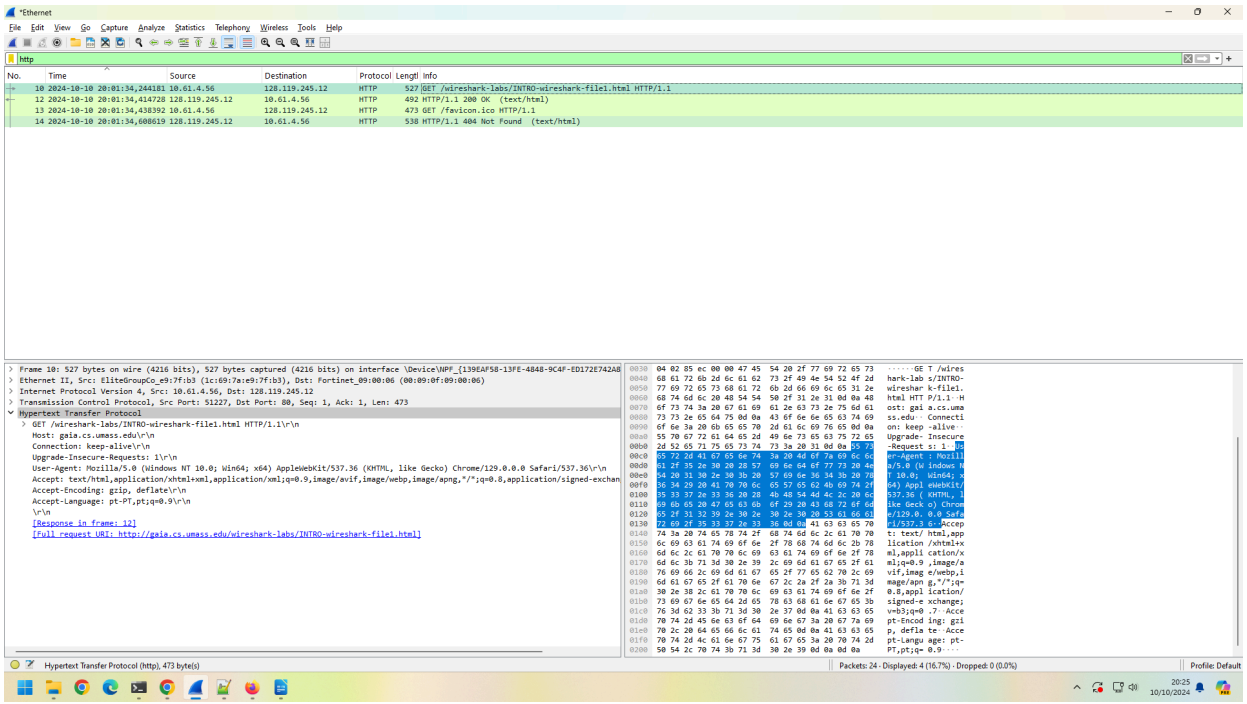
Aluno: Kauã Melchioretto, João Miguel Steffen Marchi
ADS

Laboratório Intro de Redes

1. Quais dos seguintes protocolos são mostrados como aparecendo (ou seja, estão listados na coluna “protocolo” do Wireshark) em seu arquivo de rastreamento: TCP, QUIC, HTTP, DNS, UDP, TLSv1.2?
   R: Protocolo HTTP, utilizado para baixar o HTML da página.

2. Quanto tempo demorou desde o envio da mensagem HTTP GET até o recebimento da resposta HTTP OK? (Por padrão, o valor da coluna Time na janela de listagem de pacotes é a quantidade de tempo, em segundos, desde o início do rastreamento do Wireshark. (Se você deseja exibir o campo Time no formato de hora do dia, selecione o botão Wireshark *Exibir* menu suspenso, selecione *Formato de exibição* de hora e selecione *Hora do dia*.)
   R: Não utilizei o arquivo disponibilizado, fiz manualmente, sendo assim o meu tempo de resposta foi bem diferente do disponibilizado.
   Entre a requisição do GET e o retorno HTTP 200 demoraram cerca de 200 milisegundos.
   Segue print abaixo:



3. Qual é o endereço de Internet do gaia.cs.umass.edu (também conhecido como www-net.cs.umass.edu)? Qual é o endereço de Internet do seu computador ou (se você estiver usando o arquivo de rastreamento) do computador que enviou a mensagem HTTP GET?
   R: O endereço de internet o qual foi realizado a requisição foi para o URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html

Para responder às duas perguntas a seguir, você precisará selecionar o pacote TCP que contém a solicitação HTTP GET (dica: este é o pacote número 286[1]). O objetivo dessas duas próximas perguntas é familiarizar-se com o uso da janela "Detalhes da janela de pacote selecionada" do Wireshark; veja a Figura 3. Para fazer isso, clique em Packet 286 (sua tela deve ser semelhante à Figura 3). Para responder à primeira pergunta abaixo, procure na janela “Detalhes do pacote selecionado” alterne o triângulo para HTTP (sua tela deve ficar semelhante à Figura 5); para a segunda pergunta abaixo, você precisará expandir as informações sobre a parte do Protocolo de Controle de Transmissão (TCP) deste pacote.

4. Expanda as informações sobre a mensagem HTTP na janela “Detalhes do pacote selecionado” do Wireshark (consulte a Figura 3 acima) para que você possa ver os campos na mensagem de solicitação HTTP GET. Que tipo de navegador da Web emitiu a solicitação HTTP? A resposta é mostrada na extremidade direita das informações após o campo “User-Agent:” na exibição de mensagem HTTP expandida. [Esse valor de campo na mensagem HTTP é como um servidor da Web descobre que tipo de navegador você está usando.]
R: O navegador utilizado para a requisição GET foi o: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.0.0 Safari/537.36

Laboratório de Redes HTTP (para entregar)

1. Seu navegador está executando HTTP versão 1.0, 1.1 ou 2? Qual versão do HTTP o servidor está executando?
R: Request Version: HTTP/1.1

2.Quais idiomas (se houver) seu navegador indica que pode aceitar para o servidor?
R: Accept-Language: pt-PT,pt;q=0.9\r\n

3. Qual é o endereço IP do seu computador? Qual é o endereço IP do servidor gaia.cs.umass.edu?
R: Source Address: 10.61.4.56
Destination Address: 128.119.245.12

4. Qual é o código de status retornado do servidor para o seu navegador?
R: Status Code: 200

5. Quando o arquivo HTML que você está recuperando foi modificado pela última vez no servidor?
R: Last-Modified: Thu, 10 Oct 2024 05:59:02 GMT\r\n

6. Quantos bytes de conteúdo estão sendo retornados ao seu navegador?
R: File Data: 81 bytes => Tamanho do File Data

7. Ao inspecionar os dados brutos na janela de conteúdo do pacote, você vê algum cabeçalho nos dados que não são exibidos na janela de listagem de pacotes? Em caso afirmativo, cite um.
R: O que está no lado esquerdo está representado no lado direito porém detalhado em Hexadecimal, sendo assim, o que está no lado esquerdo, está no lado direito de uma forma “codificada”. Porém há informações mais técnicas que estão por debaixo dos panos que não conseguimos ver.

1

8. Inspecione o conteúdo da primeira solicitação HTTP GET de seu navegador para o servidor. Você vê uma linha “IF-MODIFIED-SINCE” no HTTP GET?
R: Não, na primeira não é exibido, somente na segunda é exibido o dado abaixo:
If-Modified-Since: Thu, 10 Oct 2024 05:59:02 GMT\r\n

9. Inspecione o conteúdo da resposta do servidor. O servidor retornou explicitamente o conteúdo do arquivo? Como você sabe?
R: Sim, porém o conteúdo do arquivo é possível ser visto no HTTP 200, na seção “Line-based text data: text/html (10 lines). Onde há um html da página.

Line-based text data: text/html (10 lines)

10.Agora inspecione o conteúdo da segunda solicitação HTTP GET do seu navegador para o servidor. Você vê uma linha “IF-MODIFIED-SINCE:” no HTTP GET? Em caso afirmativo, quais informações seguem o cabeçalho “IF-MODIFIED-SINCE:”?
R: A informação é: If-Modified-Since: Thu, 10 Oct 2024 05:59:02 GMT\r\n.
O conteúdo é uma data em Dia da semana, dia do mês, mês, ano, hh:nn:ss GTM, resumindo, DateTime.

11. Qual é o código de status HTTP e a frase retornada do servidor em resposta a esse segundo HTTP GET? O servidor retornou explicitamente o conteúdo do arquivo? Explicar.
R: A resposta do servidor é HTTP/1.1 304 Not Modified\r\n. Não foi retornado o conteúdo explicitamente, pois não é possível localizar a seção “Line-based text data: text/html…”. Isso porque não faz sentido o servidor nos retornar um arquivo que não sofreu modificação se ele já nos retornou anteriormente, e essa resposta está no cache, já que o arquivo não foi alterado, “mantém o mesmo”.

12.Quantas mensagens de solicitação HTTP GET seu navegador enviou? Qual número de pacote no rastreamento contém a mensagem GET para o Bill ou Rights?
R: O navegador envio apenas uma requisição GET. Eu não utilizei o baixado, sendo assim, meu número estará diferente, o meu HTTP GET, na seção “Transmission Control Protocol, Src Port: 51398, Dst Port: 80, Seq: 1, Ack: 1, Len: 472” da minha requisição possuí o dado “[Next Sequence Number: 473 (relative sequence number)]”, após esse HTTP, tenho 4 pacotes TCP que foram recebidos do servidor, analisando esses pacotes TCP esses pacotes possuem uma info em comum com esse HTTP, a informação fica na mesma seção, sendo o dado “Acknowledgment Number: 473 (relative ack number)”, ambos os 4 pacotes TCP possuem esse mesmo número identificador.

13. Qual número de pacote no rastreamento contém o código de status e a frase associada à resposta à solicitação HTTP GET?
R: O n° do pacote de rastreamento é o “Acknowledgment Number: 473 (relative ack number)” do nosso retorno HTTP 200OK que o servidor nos retornou. Pois, o HTTP final, é a junção de todos os pacotes TCP enviados para formar o HTTP.

14. Qual é o código de status e a frase na resposta?
R: HTTP/1.1 200 OK\r\n

15. Quantos segmentos TCP contendo dados foram necessários para transportar a única resposta HTTP e o texto da Declaração de Direitos?
R: Foram utilizados 4 segmentos TCP para o final.

16. Quantas mensagens de solicitação HTTP GET seu navegador enviou? Para quais endereços da Internet essas solicitações GET foram enviadas?
R: 3 solicitações GET. Os endereços de internet solicitados GET foram os IPs “128.119.245.12” e “128.119.245.12”, o estranho foi que os GETs pegavam imagens porém cada um dos arquivos vem de um IP diferente que são os citados acima. O primeiro GET é solicitado para o .HTML

17. Você pode dizer se o seu navegador baixou as duas imagens em série ou se elas foram baixadas dos dois sites em paralelo? Explicar.
R: Elas foram baixadas em paralelo pois cada uma vem de um IP diferente e possui uma sequence diferente, porém é percebido que é recebido somente um HTTP OK de PNG que também vem de um IP diferente dos IPs citados na questão anterior, isso porque as imagens estão em um HTML que está em um servidor e as imagens são um SRC de outros 2 servidores que possuem a imagem, se ambas correspondessem a uma imagem única desse servidor do HTML que corresponde ao IP “192.168.1.3” seriam baixadas em série.

18. Qual é a resposta do servidor (código e frase de status) em resposta à mensagem HTTP GET inicial do seu navegador?
R: O código obtido é “401 Unauthorized” isso pois o usuário não possui autorização para acesso.

19. Quando o seu navegador envia a mensagem HTTP GET pela segunda vez, que novo campo é incluído na mensagem HTTP GET?
R: Após inserir o usuário e senha o HTTP GET obtido é HTTP 200 OK pois foi autenticado corretamente, assim, permite o acesso e retorna o arquivo HTML